World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:9, No:06, 2015

Efficient Internal Generator Based on Random Selection of an Elliptic Curve

Authors : Mustapha Benssalah, Mustapha Djeddou, Karim Drouiche

Abstract : The random number generation (RNG) presents a significant importance for the security and the privacy of numerous applications, such as RFID technology and smart cards. Since, the quality of the generated bit sequences is paramount that a weak internal generator for example, can directly cause the entire application to be insecure, and thus it makes no sense to employ strong algorithms for the application. In this paper, we propose a new pseudo random number generator (PRNG), suitable for cryptosystems ECC-based, constructed by randomly selecting points from several elliptic curves randomly selected. The main contribution of this work is the increasing of the generator internal states by extending the set of its output realizations to several curves auto-selected. The quality and the statistical characteristics of the proposed PRNG are validated using the Chi-square goodness of fit test and the empirical Special Publication 800-22 statistical test suite issued by NIST.

Keywords : PRNG, security, cryptosystem, ECC
Conference Title : ICPISL 2015 : International Conference on Privacy and Information Security Law
Conference Location : Paris, France
Conference Dates : June 25-26, 2015